STATE OF CALIFORNIA
Budget Change Proposal - Cover Sheet
DF-46 (REV 08/15)

Fiscal Year	Business Unit	Department	Priority No.
2016-17	0250	JUDICIAL BRANCH	013

Budget Request Name	Program	Subprogram
0250-013-BCP-BR-2016-GB	**0140 JUDICIAL COUNCIL**	

Budget Request Description
Information Systems Control Enhancements

Budget Request Summary
The Judicial Council requests a General Fund augmentation in Fiscal Year (FY) 2016-17 of $3.191 million for one-time costs and $1.950 million for ongoing funding in FY 2017-18 to strengthen information technology security controls and enhance the reliability of Judicial Branch data. This request also includes three full time employees to support information technology security and disaster recovery programs

Requires Legislation	Code Section(s) to be Added/Amended/Repealed	
☐ Yes ☒ No		
Does this BCP contain information technology (IT) components? ☒ Yes ☐ No *If yes, departmental Chief Information Officer must sign.*	Department CIO Mark Dusman	Date 08/27/2015

For IT requests, specify the date a Special Project Report (SPR) or Feasibility Study Report (FSR) was approved by the Department of Technology, or previously by the Department of Finance.
☐ FSR ☐ SPR Project No. Date:

If proposal affects another department, does other department concur with proposal? ☐ Yes ☐ No
Attach comments of affected department, signed and dated by the department director or designee.

Prepared By	Date	Reviewed By	Date
Michael Derr		Mark Dusman/Diana Earl	
Chief Administrative Officer Walter Throckmorton	Date 12/31/15	Administrative Director Signed for MH	Date 12/31/15

Department of Finance Use Only

Additional Review: ☐ Capital Outlay ☐ ITCU ☐ FSCU ☐ OSAE ☐ CALSTARS ☐ Dept. of Technology

BCP Type: ☐ Policy ☐ Workload Budget per Government Code 13308.05

PPBA	Date submitted to the Legislature
B. J	1/7/16

Analysis of Problem

A. Budget Request Summary

The FY 2016-17 Budget Change Proposal for the Implementation of Information Systems Control Enhancements requests $3.191 million (initial) and $1.950 million (ongoing) to strengthen information technology security controls and enhance the reliability of Judicial Branch data. Focus is needed both within the Judicial Council, and in the Judicial Council's ability to more effectively assist the trial courts in these areas. The funds requested will be used for the following information technology related items:

1) Audit and Accountability - the implementation of user access auditing tools within the courts;
2) Risk Assessment - the establishment of annual information systems risk assessments;
3) Contingency Planning - the implementation of information technology disaster recovery infrastructure and capabilities within the Judicial Council;
4) Security Program Management - the implementation of a formalized information security program within the Judicial Council; and
5) Media Protection - the preparation for the implementation of a data classification program within the Judicial Council.

This request includes three full-time employees to support information technology security and disaster recovery programs within the Judicial Council

B. Background/History *(Provide **relevant** background/history and provide program resource history. Provide workload metrics, if applicable.)*

The increasing frequency of information technology security breaches in both public and private sector organizations has demonstrated a need for the Judicial Council to review its ability to protect itself from compromise, and should a breach or infrastructure outage occur, to be able to recover effectively and in a timely manner. Focus is needed both within the Judicial Council, and in the Judicial Council's ability to more effectively assist the courts in these areas.

The National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, provides standards, guidelines and other useful security-related information which organizations can use to assess their security posture, and to implement or strengthen controls to improve their security posture. Among these publications, Special Publication 800-53 provides specific guidance in a broad range of areas including security management, access controls, configuration management, contingency planning, incident response, and more. The Judicial Council has reviewed NIST's Special Publication 800-53, and has identified five critical areas where investment is critical.

1) Audit and Accountability: NIST's Audit and Accountability controls specify the ability to (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information systems users can be uniquely traced to those users so they can be held accountable for their actions.

Item	Cost (One Time)	Cost (Ongoing)
1. Software Licensing	243,400	0
2. Software Maintenance and Support	0	46,800
3. IT Equipment	377,000	0
Total	**620,400**	**46,800**

2) Risk Assessment: The Judicial Council security framework follows NIST standards that organizations must perform periodic information technology risk assessments. For these assessments to be objective, however, they should be performed by external qualified parties. As a result, these assessments will result in costs that are unable to be covered within the Judicial Council's existing budget. Assessments are to include a review of the risk and magnitude of the harm that could result

from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the organization's operations and assets.

Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, and other organizations based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). Funding Requested: $208,000 one-time and $104,000 ongoing for the establishment of annual information systems risk assessments within the Judicial Council. Additionally, $936,000 is requested initially and ongoing for each subsequent year for the performance of risk assessments and proactive remediation efforts within the trial courts. The scope of the trial court risk assessment initiative will be restricted to smaller trial courts that have limited IT resources. The trial court costs provided below are based on providing up to 26 courts with 480 hours of effort per court on a biennial basis. Actual allocations are expected to vary within that budget based on need.

Item	Cost (One Time)	Cost (Ongoing)
1. Professional Services – Judicial Council	208,000	104,000
2. Professional Services – Trial Courts	936,000	936,000
Total	**1,144,000**	**1,040,000**

3) Contingency Planning: While the Judicial Council has partially implemented individual functions specified by this set of controls, others must still be implemented or enhanced and formalized under an ongoing disaster recovery program. This set of controls specifies the establishment of (i) procedures for protecting information resources and minimizing the risk of unplanned interruptions and (ii) a plan to recover critical operations should interruptions occur. Such plans should consider the activities performed at general support facilities, such as data processing centers and telecommunications facilities, as well as those performed by users of specific applications.

To determine whether recovery plans will work as intended, they should be tested periodically in disaster-simulation exercises. Organizations are responsible for the implementation of an information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization. Funding Requested: $540,276 one-time and $334,276 ongoing for the implementation of information technology disaster recovery infrastructure and capabilities within the Judicial Council. Also, $177,898 one-time and $167,491 ongoing is being requested for the addition of one full time Senior Business Systems Analyst to the Judicial Council staff to support contingency planning functions.

Item	Cost (One Time)	Cost (Ongoing)
1. Professional Services	156,000	0
2. Wide Area Network	141,600	141,600
3. IT Equipment	242,676	192,676
4. Staff: 1 FTE	177,898	167,491
Total	**718,174**	**501,767**

4) Security Program Management: While the Judicial Council has partially implemented individual functions specified by this set of controls, others must still be implemented or enhanced and formalized under an ongoing security program that is properly staffed and whose work assignments do not include the same development, administration and support tasks that they are responsible for monitoring and reviewing.

This set of controls specifies the need for a formalized security program within the organization. Such a program includes the establishment of a security program plan, the appointment of an Information Security Officer, and the establishment of information security resources. Additionally, measures of performance are to be established, along with a risk management strategy, insider threat program,

testing, training and monitoring capabilities, and the establishment of a threat awareness program. Funding Requested: $383,497 one-time and $361,915 ongoing for the implementation of a formalized information security program within the Judicial Council, to include the addition of one full time Information Systems Supervisor and one full time Senior Business Systems Analyst.

Item	Cost (One Time)	Cost (Ongoing)
1. Staff: 2 FTE	383,497	361,915
Total	**383,497**	**361,915**

5) Media Protection: While the Judicial Council has partially implemented individual functions specified by this set of controls, the establishment of a formalized data classification program is still outstanding. This set of controls specifies the need for specific media protection measures, which include access controls, storage and transport requirements, use restrictions, and handling of media that is commensurate with the security category and/or classification of the information residing on the media. Funding Requested: $325,000 one-time to establish the framework for the implementation of a data classification program within the Judicial Council.

Item	Cost (One Time)	Cost (Ongoing)
1. Professional Services	325,000	0
Total	**325,000**	**0**

C. State Level Considerations

This proposal aligns with the California Judicial Branch guiding principles for technology, as well as with the branch's Strategic and Tactical Plans for Technology, which provides a comprehensive and cohesive strategy with clear, measureable goals and objectives at the branch level.

- Guiding Principles: This request aligns with the following guiding technology principles as adopted by the Judicial Council.
  - Principle 6: Secure Private Information. Design services to comply with privacy laws and to assure users that personal information is properly protected.
  - Principle 7: Provide Reliable Information. Ensure the accuracy and timeliness of information provided to judges, parties, and others.
  - Principle 8: Protect from Technology Failure. Define contingencies and remedies to guarantee that users do not forfeit legal rights when technologies fail and users are unable to operate systems successfully.
  - Principle 9: Improve Court Operations. Advance court operational practices to make full use of technology and, in turn, provide better service to court users.
  - Principle 11: Improve Branch wide Compatibility through Technology Standards.
- Strategic Plan: This request aligns with goals 2 and 3 of the California Judicial Branch Strategic Plan for Technology.
  - Goal 2: Optimize Branch Resources
    - Objective 2.6. Promote continual improvement of court practices by collaborating on court technology solutions, leverage and share technology resources, and creating tools to educate court stakeholders and the public.
    - Objective 2.7. Identify and implement technology best practices within the branch.
  - Goal 3: Optimize Infrastructure
    - Objective 3.1. Ensure secure and reliable data network connectivity throughout the branch.

- Objective 3.2. Provide a consistent level of infrastructure security across the branch.
- Objective 3.5. Ensure that critical systems and infrastructure can be recovered in a timely manner after a disaster

- Tactical Plan for Technology: This request aligns with the California Judicial Branch Tactical Plan for Technology's initiatives to optimize infrastructure
  - Initiative: Court Information Systems Security Policy Framework.
    - The goal of this initiative is for every court to use the same security framework for adoption into their local information security policies. The framework provides a common reference point recognizing that local policies may not be the same among the courts. This request supports Strategic Plan Objectives 3.1 and 3.2.
  - Initiative: Court Disaster Recovery Framework and Pilot.
    - The goal of this initiative is to ensure that adequate disaster recovery provisions will be made for all systems, services, and information maintained by the judicial branch. This request supports Strategic Plan Objectives 3.1 and 3.5.

There are no known anticipated adverse impacts.

D. Justification

The security of the Judicial Branch's technology systems and the reliability of the data produced by these systems are paramount. Sustained budget cuts have left the branch with no margin to make significant investments in critical areas such as this without making cuts in other critical areas. The controls established within NIST SP 800-53 and incorporated in the Judicial Council's security framework were motivated by ever-evolving threats to security, and characterized by the increasing sophistication of cyber-attacks and the increasing frequency of these attacks. Without sufficient funding for security, the Judicial Council's ability to keep pace with these evolving threats will be impaired, and technology systems will be at a greater risk for compromise and data loss.

In regards to the specific areas where funding is being requested:

1) **Risk Assessment**: the establishment of annual information systems risk assessments within the Judicial Council is essential in ensuring that all threats and vulnerabilities to the council's information systems are identified and considered, that the greatest risks are addressed, and that appropriate decisions are made regarding which risks to accept and which to mitigate through security controls. Without an effective risk management program, the Judicial Council risks not being able to identify and address critical vulnerabilities before they result in outages, system compromise, or loss of data.

2) **Contingency Planning**: the implementation of effective information technology disaster recovery infrastructure and capabilities within the Judicial Council is critical to ensure service continuity by addressing potential disruptions. These may include relatively minor interruptions such as temporary power failures as well as major disasters such as fires, natural disasters and terrorism, all of which might require re-establishing operations at a remote location. Without an effective information technology disaster recovery program, the Judicial Council risks extended downtime and potential loss of data in the event of the loss of key systems or facilities.

3) **Security Program Management**: the implementation of a formalized and effective information security program within the Judicial Council is critical to ensure the Judicial Council's ability to implement and enforce best practices, and to keep pace with evolving threats which can impair technology systems and place the agency at a greater risk for compromise and data loss. Without funding in this area, the Judicial Council cannot adequately address the critical elements identified by NIST for an effective security management program.

4) **Media Protection**: preparations for the implementation of a data classification program within the Judicial Council are critical in that an effective data classification program provides the foundation to ensure that information is properly classified, and in turn, that the appropriate security measures to preserve the integrity, availability and required level of confidentiality of the council's information

resources. Without funding in this area, the Judicial Council risks the mishandling of data that has not been properly classified, and risks increased costs by maintaining data for longer periods than are required.

Outcomes and Accountability *(Provide summary of expected outcomes associated with Budget Request and provide the projected workload metrics that reflect how this proposal improves the metrics outlines in the Background/History Section.)*

The Judicial Council expects to see improvements in the following areas:

Using the deployment of user access auditing tools within the Judicial Council as a proof of concept, the intent is to extend this functionality to the courts via a centrally-funded program that does not divert court funding from other priorities. Trial courts will then have local tools that can collect server log data into a single location where user account changes can be identified and documented. This will give them visibility into the underlying automated logging that shows the date and time of when actual system events were processed.

1) **Risk Assessment** (the establishment of annual information systems risk assessments within the Judicial Council): The hiring of specialized external consultants on an annual basis to provide ongoing risk assessments will help determine the risk and magnitude of harm associated with unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems that support the courts operations and assets.

   Annually, these assessments will be used to monitor progress against any issues. Ongoing risk assessments would determine risk and magnitude of harm associated with unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems that support their operations and assets.

   In regards to assessments performed at trial courts, an additional focus would be provided in helping trial court executives and IT management understand what is needed to comply with security controls that have been mandated.

2) **Contingency Planning**: The establishment of a formalized disaster recovery program will ensure service continuity by addressing potential disruptions. These may include relatively minor interruptions such as temporary power failures as well as major disasters such as fires, natural disasters and terrorism, any of which might require re-establishing operations at a remote location.

3) **Security Management Program** (the implementation of a formalized information security program within the Judicial Council): The security program will improve the Judicial Council's ability to implement and enforce best practices, and to keep pace with evolving threats which can impair technology systems and place the agency at a greater risk for compromise and data loss.

4) **Media Protection** (preparations for the implementation of a data classification program within the Judicial Council): By performing a data classification study, the Judicial Council will have the necessary framework to implement a data classification program that will ensure that data is stored, labeled and safeguarded in accordance with industry standards and commensurate with its classification.

The following workload measures can be achieved if the Budget Change Proposal is approved and funding and resources are received.

Projected Outcomes

Workload Measure	CY	BY	BY+1	BY+2	BY+3	BY+4
Trial Court User Access Auditing Tool Deployment	0	1	0	0	0	0
Production of User Access Auditing Reports	0	1	1	1	1	1
Judicial Council Information Technology Risk Assessments	0	1	1	1	1	1
Trial Court Information Technology Risk Assessments	0	13	13	13	13	13

Workload Measure	CY	BY	BY+1	BY+2	BY+3	BY+4
Judicial Council Disaster Recovery Study	0	1	0	0	0	0
Performance of Periodic Disaster Recovery Tests	0	0	1	1	1	1
Judicial Council Data Classification Study	0	1	0	0	0	0
Implementation and ongoing support of Data Classification Study Recommendations	0	1	1	1	1	1
Implementation and ongoing maintenance of Judicial Council WAN Infrastructure Enhancements	0	1	1	1	1	1

F. Analysis of All Feasible Alternatives

Alternative 1

The recommended solution is to invest in the five information technology areas relating to information systems control enhancements. The total cost to fund this solution is $3.191 million in one-time funding for fiscal year 2016-17 and $1.950 million in ongoing funding.

Pros

- Courts will have local tools that will give them visibility into the underlying automated logging of actual system events.
- Ongoing risk assessments would determine risk and magnitude of harm associated with unauthorized access or destruction of data.
- Disaster recovery preparations will ensure service continuity by addressing potential scenarios. All of which might include re-establishing operations at a remote location.
- The security program will improve Judicial Council's ability to implement and enforce best practices and to keep pace with evolving threats which can impair technology systems and place the agency at greater risk.
- A properly architected data classification program will ensure that data is stored, labeled and safeguarded at a level commensurate with its classification.

Cons

- Requires additional General Fund resources.

Alternative 2

The alternate solution would be to do nothing, which would continue to leave fundamental gaps in the Judicial Council's information systems controls.

Pros

- No additional funding would be required at the current time.

Cons

- Fundamental gaps will remain in the Judicial Council's information systems controls.
- Without sufficient funding for security, the Judicial Council's ability to keep pace with these evolving threats will be impaired.
- Technology systems will be at a greater risk for compromise and data loss.
- The potential for unexpected expenses to address information security-related issues down the road is increased.

G. Implementation Plan

The implementation of the improvements that are included within this request will be performed in accordance with the California Judicial Branch's Technology Governance and Funding Model, which defines general requirements for project planning and execution. At a more detailed level, the Judicial Council's solution development lifecycle (SDLC) will govern the implementation through the initiation, planning, execution, performance & control, and closing phases.

Task	Projected Start Date	Projected Completion Date
STAFFING		
Post and Recruit Positions	1Q FY 2016-17	2Q FY 2016-17
Hire and Train	2Q FY 2016-17	3Q FY 2016-17
Procure IT Equipment and Software	2Q FY 2016-17	2Q FY 2017-17
PROGRAM DEVELOPMENT		
Retain independent consultants for Risk Assessment	1Q FY 2016-17	3Q FY 2016-17
Retain independent consultants for Disaster Recovery and Data Classification	1Q FY 2016-17	3Q FY 2016-17
Create criteria for baseline risk assessment	2Q FY 2016-17	3Q FY 2016-17
Develop disaster recovery program requirements and recovery standards	3Q FY 2016-17	4Q FY 2016-17
Complete the security program documentation	1Q FY 2016-17	3Q FY 2016-17
Determine strategy, requirements and methodology for data classification	3Q FY 2016-17	4Q FY 2016-17
IMPLEMENTATION		
Procure auditing tools for the Courts	2Q FY 2016-17	2Q FY 2016-17
Conduct baseline risk assessment	3Q FY 2016-17	4Q FY 2016-17
Publish baseline risk assessment study	4Q FY 2016-17	4Q FY 2016-17
Site DR infrastructure improvements (hardware/software/services)	1Q FY 2016-17	4Q FY 2016-17
Deployment and support for auditing tools	4Q FY 2016-17	ongoing
Conduct periodic risk assessments	4Q FY 2017-18	ongoing
Conduct periodic disaster recovery plan tests	4Q FY 2016-17	ongoing

H. Supplemental Information *(Describe special resources and provide details to support costs including appropriate back up.)*

A review of just a few of the many breaches reported in recent years underscores the criticality of making investments in information technology security, and the significant costs that can be incurred in the event of a security breach.

- June 2015 - U.S. Government Office of Personnel Management. Hackers exploited weaknesses in aging systems to gain access on 4.2 million current and former federal employees. Subsequent reports have revised the number of people affected upwards to 21.5 million, including 19.7 million people who had applied for background check investigations, and another 1.8 million people including spouses who did not apply for background checks but whose information was included in the forms. The Office of Personnel Management has provided estimates of $93 million to cover predicted costs.
- June 2014 – Montana Department of Health and Human Services. Up to 1.3 million records were compromised following the hacking of a server at Montana's public health department in May.

These records included personally identifiable information (PII) such as names, addresses, birth dates, Social Security numbers, bank account information, and in some cases, health related information.

- April 2014 - County of Los Angeles. A theft of computers containing personal information of more than 342,000 patients resulting in the compromise of patient names, Social Security numbers, billing information, dates of birth, addresses, diagnoses, and other information despite encryption policies that were already in place.
- December 2013 – Target Corp. Hackers gained access to the company's internal network and exploited weaknesses to install malware in the retailer's security and payments system that was designed to capture shopper's credit card information at approximately 1700 retail locations. Ultimately, approximately 40 million credit and debit cards were stolen. According to the firm's earning reports, the net expense of this breach thus far stands at $162 million.

I. Recommendation

Alternative 1 is the recommended solution as it provides the necessary information systems control enhancements that would improve our alignment with industry standards. The five areas that are addressed would strengthen the security controls and also work to better ensure the availability and reliability of Judicial Branch data. Additionally, alternative 1 supports the California Judicial Branch guiding principles for technology, as well as with the branch's Strategic and Tactical Plans for Technology.

BCP Fiscal Detail Sheet

BCP Title: Information Systems Control Enhancements

DP Name: 0250-013-BCP-DP-2016-GB

Budget Request Summary

	FY16					
	CY	BY	BY+1	BY+2	BY+3	BY+4
Positions - Permanent	0.0	3.0	3.0	3.0	3.0	3.0
Total Positions	**0.0**	**3.0**	**3.0**	**3.0**	**3.0**	**3.0**
Salaries and Wages						
Earnings - Permanent	0	307	307	307	307	307
Total Salaries and Wages	**$0**	**$307**	**$307**	**$307**	**$307**	**$307**
Total Staff Benefits	0	150	150	150	150	150
Total Personal Services	**$0**	**$457**	**$457**	**$457**	**$457**	**$457**
Operating Expenses and Equipment						
539X - Other	0	2,734	1,493	1,493	1,493	1,493
Total Operating Expenses and Equipment	**$0**	**$2,734**	**$1,493**	**$1,493**	**$1,493**	**$1,493**
Total Budget Request	**$0**	**$3,191**	**$1,950**	**$1,950**	**$1,950**	**$1,950**

Fund Summary

Fund Source - State Operations						
0001 - General Fund	0	3,191	1,950	1,950	1,950	1,950
Total State Operations Expenditures	**$0**	**$3,191**	**$1,950**	**$1,950**	**$1,950**	**$1,950**
Total All Funds	**$0**	**$3,191**	**$1,950**	**$1,950**	**$1,950**	**$1,950**

Program Summary

Program Funding						
0140010 - Judicial Council	0	3,191	1,950	1,950	1,950	1,950
Total All Programs	**$0**	**$3,191**	**$1,950**	**$1,950**	**$1,950**	**$1,950**

Personal Services Details

Positions	Salary Information Min	Mid	Max	CY	BY	BY+1	BY+2	BY+3	BY+4
VR00 - Various (Eff. 07-01-2016)				0.0	3.0	3.0	3.0	3.0	3.0
Total Positions				**0.0**	**3.0**	**3.0**	**3.0**	**3.0**	**3.0**

Salaries and Wages	CY	BY	BY+1	BY+2	BY+3	BY+4
VR00 - Various (Eff. 07-01-2016)	0	307	307	307	307	307
Total Salaries and Wages	**$0**	**$307**	**$307**	**$307**	**$307**	**$307**
Staff Benefits						
5150900 - Staff Benefits - Other	0	150	150	150	150	150
Total Staff Benefits	**$0**	**$150**	**$150**	**$150**	**$150**	**$150**
Total Personal Services	**$0**	**$457**	**$457**	**$457**	**$457**	**$457**